From: Robert Morgester via California District Attorneys Association
To: dmcclive@bakersfieldpd.us
Subject: eCrimes : Dec 2018 NAGTRI Cybercrime News
Date: Tuesday, December 18, 2018 10:51:22 AM

eCrimes

Post New Message

Reply to Group | Reply to Sender

Dec 18, 2018 1:51 PM
Robert Morgester

The following is a compendium of news reports, case law and legislative actions over the latest bi-monthly period that may be of interest to our AG offices that are dealing with cyber-related issues.

Email not displaying correctly?
View Online | *Send to a Friend*

The following is a compendium of news reports, case law and legislative actions over the latest bi-monthly period that may be of interest to our AG offices that are dealing with cyber-related issues. Neither the National Association of Attorneys General nor the National Attorneys General Training & Research Institute expresses a view as to the accuracy of news accounts, nor as to the position expounded by the authors of the hyperlinked articles.

December 2018

Recent Developments of Note

The U.S. House Energy and Commerce Subcommittee on Oversight and Investigations released a cybersecurity strategy report which suggests that companies need to revamp how they find and fix vulnerabilities in their Internet-connected devices. The report also highlights the priorities for the

subcommittee in the upcoming year.

The U.S. District Court for the Southern District of California denied the SEC's request for a preliminary injunction against cryptocurrency startup Blockvest, which was alleged to have planned to fraudulently raise money in an initial coin offering. The court found the SEC had failed to show that investors who bought into Blockvest were buying securities.

Delta Air Lines launched its first facial recognition terminal at Atlanta International Airport. The program is optional, and any passenger who does not want to use the system can go through the usual ID verification process. Also at Atlanta Airport, Hertz opened a biometric car rental lane to speed up the rental process, with plans to roll it out to 40 other airport locations within the next year.

Recent State Cases of Interest

In Pohland v. State, an Alaska appeals court ruled that the search of defendant's laptop violated the Fourth Amendment, and therefore the evidence against her obtained as a result of that search should have been suppressed because the search warrant did not show that the officers had probable cause to believe the documents relating to the finances of defendant's landlord would be found on the laptop. AAG Michal Stryzak represented the State.

In Ferrari v. State, a Florida appeals court found that defendant's motion to suppress cell phone site data should have been denied because it was obtained without a warrant based on probable cause, and the good faith exception to the exclusionary rule did not apply because the State was not relying on binding precedent or clearly applicable statutes in obtaining the data. AAG Melanie Surber represented the State.

In Agnew v. State, the Maryland Court of Appeals held that an audio-recorded conversation recovered from the defendant's cell phone was properly admitted under the Wiretap Act because the defendant knowingly and intentionally recorded himself and another person on his phone, deliberately violating the Act, and the defendant lacked a reasonable expectation of privacy in his conversation. AAG Brenda Gruss represented the State.

In State v. Andrews, a New Jersey Superior Court Appellate Division ruled that the trial court's order compelling the defendant to disclose his passcodes for his cell phones did not violate his Fifth Amendment rights, and although the defendant's act of producing the passcodes conveyed implicit facts as to the ownership, control and ability to access the phones, the conveyance of these facts was a foregone conclusion because the defendant did not give the State any information it did not already possess.

In State v. Ryan, an Ohio appeals court found that defendant's 44 convictions for pandering obscenity involving a minor and 36 convictions for pandering

sexually oriented material involving a minor were not subject to merger because each count represented an image or video, constituting a separate offense, and a separate animus existed every time a separate image or file was downloaded or saved on defendant's computer.

In Commonwealth v. Glass, a Pennsylvania Superior Court found that a GPS locator was properly used without a warrant because it was consensually placed on the confidential informant's person, not the defendant's car, so it was not a tracking device within the meaning of the statute.

In Howard v. State, a Texas appellate court ruled that the defendant, a sex offender parolee in possession of a contraband mobile phone at a half-way house that prohibited its possession, did not have a reasonable expectation of privacy in his phone's contents, although the certificate of mandatory supervision and the rules of the half-way house did not explicitly authorize the search of the phone's contents.

In State v. Pinder, the Wisconsin Supreme Court ruled that a search warrant issued for the use of a GPS tracking device on a motor vehicle, but not executed within five days after its issuance, was not void, because it was not a warrant issued for the purpose of seizing property and was not subject to the execution and return provisions of the statute. The State's brief was filed by Solicitor General Micha Tseytin.

Recent Federal Cases of Interest

In U.S. v. Terry, the Fourth Circuit ruled that the defendant's intervening act of speeding was not sufficient to purge the taint of the warrantless GPS search.

In U.S. v. Lopez-Zuniga, the Eighth Circuit ruled that evidence obtained from a GPS placed on defendant's car was properly suppressed because the first search warrant was not supported by probable cause and the good faith exception to the exclusionary rule did not apply, as allegations in the search warrant application that defendant picked up someone appearing to be a suspected drug dealer did not connect the defendant to any of the suspect's alleged illicit activities.

Cyber Initiatives in the Attorney General Community

Forty-three Attorneys General sent a letter to the Social Security Administration, asking the Acting Commissioner to prioritize the implementation of a new database system that would verify consumers' information and help prevent synthetic identity fraud.

Hedda Litwin is the Editor of the *Cybercrime Newsletter* and may be reached at 202-326-6022.The *Cybercrime Newsletter* is a publication of the National Association of Attorneys General. Any use and/or copies of this newsletter in whole or part must include the customary bibliographic citation. NAAG retains copyright and all other intellectual property rights in the material presented in this publication. For content submissions or to contact the editor directly, please e-mail hlitwin@naag.org.

Research & Newsletters **Course Catalog** **Publications**

About NAGTRI

The National Attorneys General Training & Research Institute, known as NAGTRI, was created in 2007 and serves as the research and training arm of the National Association of Attorneys General (NAAG). **NAGTRI's mission** is to provide high quality, responsive, and innovative training to state and territorial attorneys general offices.

1850 M Street NW, 12th floor, Washington DC 20036
Copyright © 2015 NAAG. All Rights Reserved.
Opt Out | Unsubscribe

Robert Morgester
SAAG eCrime Unit
Attorney General's Office
(916) 210-7251

Reply to Group Online **Reply to Group via Email** **View Thread**

Recommend **Forward**

You are subscribed to "eCrimes" as dmcclive@bakersfieldpd.us. ©California District Attorneys Association. To change your subscriptions, go to My Subscriptions. To unsubscribe from this community discussion, go to Unsubscribe.